19. DOKtreff - jeden Monat drei neue Ideen!
30.09.2021 / 17:30 - 18:30 Uhr

17:30 Uhr: Begrüßung
Ronald Senft| Medienanstalt Rheinland-Pfalz

17:35 – 17:45 Uhr: Die Flutkatastrophe und das AHRTALRADIO
Marius Reichert | Moderator, Reporter, Live-Reporter WDR

Der WDR-Live Reporter Marius Reichert berichtet von seinen Eindrücken aus dem Flutgebiet und über seine ehrenamtliche Mitarbeit beim AHRTALRADIO.

17:50 -18:00 Uhr: IT-Angriff auf die Sendetechnik von OK4
Dominika Skiba| OK4 Koblenz

Die Ransomware-Welle, die von Lösegelderpressern angetrieben wird, schwappt unverändert über Unternehmen und Behörden hinweg und gefühlt verschärft sich die Sicherheitslage. Der OK4 wurde ebenfalls Opfer einer Ransomware-Attacke und war drei Monate nahezu lahm gelegt. Dominik Skiba berichtet, wie der OK4 mit Hilfe der ehrenamtlichen sowie hauptamtlichen Techniker wieder alles in den Griff bekommen hat.

Folgende Maßnahmen sollten bei einem Ransomware-Angriff durchgeführt werden:

1. Geräte schnell isolieren.
Eine Ransomware sollte sich nicht weiter ausbreiten können, als bereits geschehen. Daher sollten Administratoren betroffene Systeme so schnell wie möglich vom Netzwerk isolieren. Vor allem bei den Aufräumarbeiten nach der Ransomware-Attacke gilt es zu verhindern, dass sich die erpresserische Malware weiter ausbreitet.

2. Den Angriffsvektor verstehen.
Sind die betroffenen Geräte isoliert, ist es wichtig zu verstehen, wie es zu dem Vorfall kommen konnte. Das hilft zum einem, den Vorfall zu bewältigen. Zudem liefert es wertvolle Lektionen für die Zukunft. Es gilt also herauszufinden: Wer war Patient Zero im Netzwerk?

3. Backups sichern und überprüfen.
Applikationen und Server lassen sich wieder einrichten, Daten sind aber unersetzlich. Ohne Backups ist es nicht mehr möglich, sie sicherzustellen. Deshalb gilt als Maßnahme, sie erst einmal vom Netz zu nehmen.
Angreifer suchen als Teil ihres Angriffs gezielt nach Backups. Sind diese weiter online, besteht die Gefahr, dass sie in den Angriff einbezogen werden. Noch besser ist es natürlich, von Offline-Backups an einem physikalisch getrennten Ort vorzuhalten. Die 3-2-1-Regel des Backups ist gerade für das Sichern von Daten gegen erpresserische Angriffe eine Selbstverständlichkeit. Damit läuft eine Lösegeldforderung unter Umständen -zumindest was den Datenbestand trifft – ins Leere. IT-Administratoren können sich stattdessen darum kümmern, die Systeme wieder aufzubauen.

4. Projekte und geplante Aufgaben stoppen.
Eine Ransomware-Attacke ist ein Notfall und erfordert das Bündeln aller Ressourcen. Ein Umbau der der IT-Architektur, wie Migrationen auf neue Umgebungen, oder das Installieren neuer Applikationen und Server sollten sofort gestoppt werden. Solche Projekte könnten der Malware helfen, sich weiter auszubreiten. Ebenso wichtig ist es, terminierte Aufgaben, zum Beispiel Backups, zu stoppen. Denn in deren Verlauf kann sich die erpresserische Malware weiter ausbreiten.

5. Potenziell kompromittierte Bereiche unter Quarantäne stellen.
Generell sollte man direkt nach einem Angriff keine Möglichkeit ausschließen und alle potenziell betroffenen Teile der Infrastruktur unter Quarantäne stellen. Das heißt, alles erst einmal vom Netz nehmen und einzeln untersuchen, bevor es wieder zum Einsatz kommen kann.

6. Nach dem Angriff ist vor dem Angriff: Passwörter ändern.
Vorsicht ist besser als Nachsicht. Zu Beginn eines Vorfalls ist oft noch nicht komplett klar, wie es dazu kommen konnte. War es lediglich ein einfacher Angriff? Oder handelte es sich um eine komplexe Attacke, die möglich war, weil der Angreifer Authentifikationsdaten erbeutet hatte? Wenn dem so war, kann er immer wieder den nächsten Versuch starten. Es ist daher auf jeden Fall sinnvoll, die Passwörter systemkritischer Nutzerkonten zu ändern.

7. Keine Panik – Kritische Sicherheitssituationen planen und üben
Die IT-Administration wird im Fall des Falles unter hohen Druck stehen – und damit besteht die Gefahr, dass in dieser Drucksituation falsch entschieden wird. Um dies möglichst zu verhindern, sollten sich IT-Abteilungen auf den Ernstfall vorbereiten. Im Idealfall haben die Sicherheitsverantwortlichen Prozesse definiert. Denn gerade im Ernstfall benötigen Unternehmen eine Blaupause, um keine sinnvollen Maßnahmen zu vergessen. Diese

Prozesse sollten außerdem regelmäßig geübt werden, so im Rahmen von simuliertem „Red and Blue Team Testing“. Wissen Mitarbeiter, dass es einen Plan gibt, der im Ernstfall greift, und dass dieser Plan geübt wurde, wird das Risiko unter Druck falsch zu handeln, minimiert.

[Quelle: https://www.zdnet.de/88396234/keine-panik-nach-ransomware-angriff/]

18:05 -18:15 Uhr: **Vertreibung aus dem Paradies**
Victoria Kretzler | FSJ rheinlOKal Speyer
Anton Kramer | FSJ OK Weinstraße – Studio Landau
Max Idler | FSJ rheinlOKal Worms

Victoria Kretzler, Anton Kramer und Max Idler erklären, wie sie in das neue FSJ gestartet sind und wie der erste TV-Bericht „Vertreibung aus dem Paradies“ entstanden ist.

Nächster Termin:
DOKtreff - jeden Monat drei neue Ideen! am Do. 28.10.2021 um 17:30 Uhr.
Online-Anmeldung unter:
https://www.bz-bm.de/seminare/5500/